PUBLIC-KEY SIGNATURE METHODS AND SYSTEMS

FIELD OF THE INVENTION

The present invention generally relates to cryptography, and more particularly to public-key cryptography.

BACKGROUND OF THE INVENTION

The first public-key cryptography scheme was introduced in 1975. Since then, many public-keys schemes have been developed and published. Many public-key schemes require some arithmetic computations modulo an integer n, where today n is typically between 512 and 1024 bits.

Due to the relatively large number of bits n, such public-key schemes are relatively slow in operation and are considered heavy consumers of random-access-memory (RAM) and other computing resources. These problems are particularly acute in applications in which the computing resources are limited, such as smart card applications. Thus, in order to overcome these problems, other families of public-key schemes which do not require many arithmetic computations modulo n have been developed. Among these other families are schemes where the public-key is given as a set of k multivariable polynomial equations over a finite mathematical field K which is relatively small, e.g., between 2 and 2^{64}.

The set of k multivariable polynomial equations can be written as follows:

$$y_1 = P_1(x_1,...,x_n)$$
$$y_2 = P_2(x_1,...,x_n)$$
$$\vdots$$
$$y_k = P_k(x_1,...,x_n),$$

where $P_1,..., P_K$ are multivariable polynomials of small total degree, typically, less than or equal to 8, and in many cases, exactly two.

Examples of such schemes include the C* scheme of T. Matsumoto and H. Imai, the HFE scheme of Jacques Patarin, and the basic form of the "Oil and Vinegar" scheme of Jacques Patarin.

The C* scheme is described in an article titled "Public Quadratic Polynomial-tuples for Efficient Signature Verification and Message-encryption" in Proceedings of EUROCRYPT'88, Springer-Verlag, pp. 419 - 453. The HFE scheme is described in an article titled "Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP): Two New Families of Asymmetric Algorithms" in Proceedings of EUROCRYPT'96, Springer-Verlag, pp. 33 - 48. The basic form of the "Oil and Vinegar" scheme of Jacques Patarin is described in an article titled "The Oil and Vinegar Signature Scheme" presented at the Dagstuhl Workshop on Cryptography in September 1997.

However, the C* scheme and the basic form of the "Oil and Vinegar" scheme have been shown to be insecure in that cryptanalysis of both the C* scheme and the basic form of the "Oil and Vinegar" scheme have been discovered and published by Aviad Kipnis and Adi Shamir in an article titled "Cryptanalysis of the Oil and Vinegar Signature Scheme" in Proceedings of CRYPTO'98, Springer-Verlag LNCS n°1462, pp. 257 - 266. Weaknesses in construction of the HFE scheme have been described in two unpublished articles titled "Cryptanalysis of the HFE Public Key Cryptosystem" and "Practical Cryptanalysis of the Hidden Fields Equations (HFE)", but at present, the HFE

scheme is not considered compromised since for well chosen and still reasonable parameters, the number of computations required to break the HFE scheme is still too large.

Some aspects of related technologies are described in the following publications:

US Patent 5,263,085 to Shamir describes a new type of digital signature scheme whose security is based on the difficulty of solving systems of k polynomial equations in m unknowns modulo a composite n; and

US Patent 5,375,170 to Shamir describes a novel digital signature scheme which is based on a new class of birational permutations which have small keys and require few arithmetic operations.

The disclosures of all references mentioned above and throughout the present specification are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

The present invention seeks to improve security of digital signature cryptographic schemes in which the public-key is given as a set of k multivariable polynomial equations, typically, over a finite mathematical field K. Particularly, the present invention seeks to improve security of the basic form of the "Oil and Vinegar" and the HFE schemes. An "Oil and Vinegar" scheme which is modified to improve security according to the present invention is referred to herein as an unbalanced "Oil and Vinegar" (UOV) scheme. An HFE scheme which is modified to improve security according to the present invention is referred to herein as an HFEV scheme.

In the present invention, a set S1 of k polynomial functions is supplied as a public-key. The set S1 preferably includes the functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, and $y_1,...,y_k$ are k variables of a second

type. The set S1 is preferably obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$. It is appreciated that the secret key operation may include a secret affine transformation s on the n+v variables $a_1,...,a_{n+v}$.

When a message to be signed is provided, a hash function may be applied on the message to produce a series of k values $b_1,...,b_k$. The series of k values $b_1,...,b_k$ is preferably substituted for the variables $y_1,...,y_k$ of the set S2 respectively so as to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),..., P''_k(a_1,...,a_{n+v})$. Then, v values $a'_{n+1},...,a'_{n+v}$ may be selected for the v "vinegar" variables $a_{n+1},...,a_{n+v}$, either randomly or according to a predetermined selection algorithm.

Once the v values $a'_{n+1},...,a'_{n+v}$ are selected, a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,..., P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ is preferably solved to obtain a solution for $a'_1,...,a'_n$. Then, the secret key operation may be applied to transform $a'_1,...,a'_{n+v}$ to a digital signature $e_1,...,e_{n+v}$.

The generated digital signature $e_1,...,e_{n+v}$ may be verified by a verifier which may include, for example, a computer or a smart card. In order to verify the digital signature, the verifier preferably obtains the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key. Then, the verifier may apply the hash function on the message to produce the series of k values $b_1,...,b_k$. Once the k values $b_1,...,b_k$ are produced, the verifier preferably verifies the digital signature by verifying that the equations $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,..., P_k(e_1,...,e_{n+v}, b_1,...,b_k)=0$ are satisfied.

There is thus provided in accordance with a preferred embodiment of the present invention a digital signature cryptographic method including the steps of supplying a set S1 of k polynomial functions as a public-key, the set S1 including the functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k,

v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, $y_1,...,y_k$ are k variables of a second type, and the set S1 is obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ where $a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$, providing a message to be signed, applying a hash function on the message to produce a series of k values $b_1,...,b_k$, substituting the series of k values $b_1,...,b_k$ for the variables $y_1,...,y_k$ of the set S2 respectively to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),...,\ P''_k(a_1,...,a_{n+v})$, selecting v values $a'_{n+1},...,a'_{n+v}$ for the v "vinegar" variables $a_{n+1},...,a_{n+v}$, solving a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,...,\ P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ to obtain a solution for $a'_1,...,a'_n$, and applying the secret key operation to transform $a'_1,...,a'_{n+v}$ to a digital signature $e_1,...,e_{n+v}$.

Preferably, the method also includes the step of verifying the digital signature. The verifying step preferably includes the steps of obtaining the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key, applying the hash function on the message to produce the series of k values $b_1,...,b_k$, and verifying that the equations $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,...,\ P_k(e_1,...,e_{n+v},\ b_1,...,b_k)=0$ are satisfied.

The secret key operation preferably includes a secret affine transformation s on the n+v variables $a_1,...,a_{n+v}$.

Preferably, the set S2 includes the set f(a) of k polynomial functions of the HFEV scheme. In such a case, the set S2 preferably includes an expression including k functions that are derived from a univariate polynomial. The univariate polynomial preferably includes a univariate polynomial of degree less than or equal to 100,000.

Alternatively, the set S2 includes the set S of k polynomial functions of the UOV scheme.

The supplying step may preferably include the step of selecting the number v of "vinegar" variables to be greater than the number n of "oil" variables. Preferably, v is selected such that q^v is greater than 2^{32}, where q is the number of elements of a finite field K.

In accordance with a preferred embodiment of the present invention, the supplying step includes the step of obtaining the set S1 from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized by that all coefficients of components involving any of the $y_1,\ldots,y_k$ variables in the k polynomial functions $P'_1(a_1,\ldots,a_{n+v},y_1,\ldots,y_k),\ldots,P'_k(a_1,\ldots,a_{n+v},y_1,\ldots,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

Preferably, the set S2 includes the set S of k polynomial functions of the UOV scheme, and the number v of "vinegar" variables is selected so as to satisfy one of the following conditions: (a) for each characteristic p other than 2 of a field K in an "Oil and Vinegar" scheme of degree 2, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, (b) for p = 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n*(1 + sqrt(3)) and lower than or equal to $n^3/6$, and (c) for each p other than 2 in an "Oil and Vinegar" scheme of degree 3, v is greater than n and lower than or equal to n^4. Preferably, the number v of "vinegar" variables is selected so as to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2.

There is also provided in accordance with a preferred embodiment of the present invention an improvement of an "Oil and Vinegar" signature method, the improvement including the step of using more "vinegar" variables than "oil" variables. Preferably, the number v of "vinegar" variables is selected so as to satisfy one of the following conditions: (a) for each characteristic p other than 2 of a field K and for a degree 2 of the "Oil and Vinegar" signature method, v satisfies the inequality $q^{(v-n)-1} * n^4 > 2^{40}$, (b) for p = 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than n*(1 + sqrt(3)) and lower

than or equal to $n^3/6$, and (c) for each p other than 2 and for a degree 3 of the "Oil and Vinegar" signature method, v is greater than n and lower than or equal to n^4. Preferably, the number v of "vinegar" variables is selected so as to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$ for a characteristic p=2 of a field K in an "Oil and Vinegar" scheme of degree 2.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Fig. 1 is a simplified block diagram illustration of a preferred implementation of a system for generating and verifying a digital signature to a message, the system being constructed and operative in accordance with a preferred embodiment of the present invention;

Fig. 2A is a simplified flow chart illustration of a preferred digital signature cryptographic method for generating a digital signature to a message, the method being operative in accordance with a preferred embodiment of the present invention; and

Fig. 2B is a simplified flow chart illustration of a preferred digital signature cryptographic method for verifying the digital signature of Fig. 2A, the method being operative in accordance with a preferred embodiment of the present invention.

Appendix I is an article by Aviad Kipnis, Jacques Patarin and Louis Goubin submitted for publication by Springer-Verlag in Proceedings of EUROCRYPT'99, the article describing variations of the UOV and the HFEV schemes.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Reference is now made to Fig. 1 which is a simplified block diagram illustration of a preferred implementation of a system 10 for generating and verifying a digital signature to a message, the system 10 being constructed and operative in accordance with a preferred embodiment of the present invention.

Preferably, the system 10 includes a computer 15, such as a general purpose computer, which communicates with a smart card 20 via a smart card reader 25. The computer 15 may preferably include a digital signature generator 30 and a digital signature verifier 35 which may communicate data via a communication bus 40. The smart card 20 may preferably include a digital signature generator 45 and a digital signature verifier 50 which may communicate data via a communication bus 55.

It is appreciated that in typical public-key signature scheme applications, a signer of a message and a receptor of a signed message agree on a public-key which is published, and on a hash function to be used. In a case that the hash function is compromised, the signer and the receptor may agree to change the hash function. It is appreciated that a generator of the public-key need not be the signer or the receptor.

Preferably, the digital signature verifier 35 may verify a signature generated by one of the digital signature generator 30 and the digital signature generator 45. Similarly, the digital signature verifier 50 may verify a signature generated by one of the digital signature generator 30 and the digital signature generator 45.

Reference is now made to Fig. 2A which is a simplified flow chart illustration of a preferred digital signature cryptographic method for generating a digital signature to a message in a first processor (not shown), and to Fig. 2B which is a simplified flow chart illustration of a preferred digital signature

cryptographic method for verifying the digital signature of Fig. 2A in a second processor (not shown), the methods of Figs. 2A and 2B being operative in accordance with a preferred embodiment of the present invention.

It is appreciated that the methods of Figs. 2A and 2B may be implemented in hardware, in software or in a combination of hardware and software. Furthermore, the first processor and the second processor may be identical. Alternatively, the method may be implemented by the system 10 of Fig. 1 in which the first processor may be comprised, for example, in the computer 15, and the second processor may be comprised in the smart card 20, or vice versa.

The methods of Fig. 2A and 2B, and applications of the methods of Figs. 2A and 2B are described in Appendix I which is incorporated herein. The applications of the methods of Figs. 2A and 2B may be employed to modify the basic form of the "Oil and Vinegar" scheme and the HFE scheme thereby to produce the UOV and the HFEV respectively.

Appendix I includes an unpublished article by Aviad Kipnis, Jacques Patarin and Louis Goubin submitted for publication by Springer-Verlag in Proceedings of EUROCRYPT'99 which is scheduled on 2 - 6 May 1999. The article included in Appendix I also describes variations of the UOV and the HFEV schemes with small signatures.

In the digital signature cryptographic method of Fig. 2A, a set S1 of k polynomial functions is preferably supplied as a public-key (step 100) by a generator of the public-key (not shown) which may be, for example, the generator 30 of Fig. 1, the generator 45 of Fig. 1, or an external public-key generator (not shown).

The set S1 preferably includes the functions $P_1(x_1,...,x_{n+v}, y_1,...,y_k),..., P_k(x_1,...,x_{n+v}, y_1,...,y_k)$, where k, v, and n are integers, $x_1,...,x_{n+v}$ are n+v variables of a first type, and $y_1,...,y_k$ are k variables of a second type. The set S1 is preferably obtained by applying a secret key operation on a set S2 of k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ where

$a_1,...,a_{n+v}$ are n+v variables which include a set of n "oil" variables $a_1,...,a_n$, and a set of v "vinegar" variables $a_{n+1},...,a_{n+v}$. It is appreciated that the secret key operation may include a secret affine transformation s on the n+v variables $a_1,...,a_{n+v}$.

The terms "oil" variables and "vinegar" variables refer to "oil" variables and "vinegar" variables as defined in the basic form of the "Oil and Vinegar" scheme of Jacques Patarin which is described in the above mentioned article titled "The Oil and Vinegar Signature Scheme" presented at the Dagstuhl Workshop on Cryptography in September 1997.

Preferably, when a message to be signed is provided (step 105), a signer may apply a hash function on the message to produce a series of k values $b_1,...,b_k$ (step 110). The signer may be, for example, the generator 30 or the generator 45 of Fig. 1. The series of k values $b_1,...,b_k$ is preferably substituted for the variables $y_1,...,y_k$ of the set S2 respectively so as to produce a set S3 of k polynomial functions $P''_1(a_1,...,a_{n+v}),..., P''_k(a_1,...,a_{n+v})$ (step 115). Then, v values $a'_{n+1},...,a'_{n+v}$ may be randomly selected for the v "vinegar" variables $a_{n+1},...,a_{n+v}$ (step 120). Alternatively, the v values $a'_{n+1},...,a'_{n+v}$ may be selected according to a predetermined selection algorithm.

Once the v values $a'_{n+1},...,a'_{n+v}$ are selected, a set of equations $P''_1(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0,..., P''_k(a_1,...,a_n,a'_{n+1},...,a'_{n+v})=0$ is preferably solved to obtain a solution for $a'_1,...,a'_n$ (step 125). Then, the secret key operation may be applied to transform $a'_1,...,a'_{n+v}$ to a digital signature $e_1,...,e_{n+v}$ (step 130).

The generated digital signature $e_1,...,e_{n+v}$ may be verified according to the method described with reference to Fig. 2B by a verifier of the digital signature (not shown) which may include, for example, the verifier 35 or the verifier 50 of Fig. 1. In order to verify the digital signature, the verifier preferably obtains the signature $e_1,...,e_{n+v}$, the message, the hash function and the public key (step 200). Then, the verifier may apply the hash function on the message to produce the series of k values $b_1,...,b_k$ (step 205). Once the k values $b_1,...,b_k$ are

produced, the verifier preferably verifies the digital signature by verifying that the equations $P_1(e_1,...,e_{n+v},b_1,...,b_k)=0,..., P_k(e_1,...,e_{n+v}, b_1,...,b_k)=0$ are satisfied (step 210).

It is appreciated that the generation and verification of the digital signature as mentioned above may be used for the UOV by allowing the set S2 to include the set S of k polynomial functions of the UOV scheme as described in Appendix I. Alternatively, the generation and verification of the digital signature as mentioned above may be used for the HFEV by allowing the set S2 to include the set f(a) of k polynomial functions of the HFEV scheme as described in Appendix I.

As mentioned in Appendix I, the methods of Figs. 2A and 2B enable obtaining of digital signatures which are typically smaller than digital signatures obtained in conventional number theoretic cryptography schemes, such as the well known RSA scheme.

In accordance with a preferred embodiment of the present invention, when the set S2 includes the set S of k polynomial functions of the UOV scheme, the set S1 may be supplied with the number v of "vinegar" variables being selected to be greater than the number n of "oil" variables. Preferably, v may be also selected such that q^v is greater than 2^{32}, where q is the number of elements of a finite field K over which the sets S1, S2 and S3 are provided.

Further preferably, the S1 may be obtained from a subset S2' of k polynomial functions of the set S2, the subset S2' being characterized by that all coefficients of components involving any of the $y_1,...,y_k$ variables in the k polynomial functions $P'_1(a_1,...,a_{n+v},y_1,...,y_k),...,P'_k(a_1,...,a_{n+v},y_1,...,y_k)$ are zero, and the number v of "vinegar" variables is greater than the number n of "oil" variables.

In the basic "Oil and Vinegar" scheme, the number v of "vinegar" variables is chosen to be equal to the number n of "oil" variables. For such a

selection of the v variables, Aviad Kipnis, who is one of the inventors of the present invention, and Adi Shamir have shown, in the above mentioned Proceedings of CRYPTO 98, Springer, LNCS n°1462, on pages 257 - 266, a cryptanalysis of the basic "Oil and Vinegar" signature scheme which renders the basic "Oil and Vinegar" scheme insecure. Additionally, by applying the same method described by Kipnis and Shamir, the basic "Oil and Vinegar" scheme may be shown to be insecure for any number v of "vinegar" variables which is lower than the number n of "oil" variables.

The inventors of the present invention have found, as described in Appendix I, that if the "Oil and Vinegar" scheme is made unbalanced by modifying the "Oil and Vinegar" scheme so that the number v of "vinegar" variables is greater than the number n of "oil" variables, a resulting unbalanced "Oil and Vinegar" (UOV) scheme may be secure.

Specifically, for a UOV of degree 2 and for all values of p other than 2, where p is a characteristic of the field K, p being the additive order of 1, the UOV scheme is considered secure for values of v which satisfy the inequality $q^{(v-n)-1} * n^4 > 2^{40}$. For a UOV of degree 2 and for p=2, the number v of "vinegar" variables may be selected so as to satisfy the inequalities $v<n^2$ and $q^{(v-n)-1} * n^4 > 2^{40}$. It is appreciated that for values of v which are higher than $n^2/2$ but less than or equal to n^2, the UOV is also considered secure, and solving the set S1 is considered to be as difficult as solving a random set of k equations. For values of v which are higher than n^2, the UOV is believed to be insecure.

Furthermore, for a UOV of degree 3 and for p = 2, the UOV scheme is considered secure for values of v which are substantially greater than n*(1 + sqrt(3)) and lower than or equal to $n^3/6$. It is appreciated that for values of v which are higher than $n^3/6$ but lower than or equal to $n^3/2$, the UOV is also considered secure, and solving the set S1 is considered to be as difficult as solving a random set of k equations. For values of v which are higher than $n^3/2$,

and for values of v which are lower than n*(1 + sqrt(3)), the UOV is believed to be insecure.

Additionally, for a UOV of degree 3 and for p other than 2, the UOV scheme is considered secure for values of v which are substantially greater than n and lower than or equal to n^4. It is appreciated that for values of v which are higher than $n^3/6$ but lower than or equal to n^4, the UOV is also considered secure, and solving the set S1 is considered to be as difficult as solving a random set of k equations. For values of v which are higher than n^4, and for values of v which are lower than n, the UOV is believed to be insecure.

Preferably, in a case that the set S2 includes the set f(a) of k polynomial functions of the HFEV scheme, the set S2 may include an expression which includes k functions that are derived from a univariate polynomial. Preferably, the univariate polynomial may include a polynomial of degree less than or equal to 100,000 on an extension field of degree n over K.

Example of parameters selected for the UOV and the HFEV schemes are shown in Appendix I.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow.